Section 1

Commitment Schemes

Commitment Schemes

Digital analogue of a safe.

Definition 1 (Commitment scheme)

An efficient two-stage protocol (S, R) .

Commit The sender S has private input $b \in \{0,1\}^*$ and the common input is 1^n. The commitment stage result in a joint output c, the *commitment*, and a private output d to S, the *decommitment*.

Reveal S sends the pair (d, b) to R, and R either accepts or rejects.

Completeness: R always accepts in an honest execution.

Hiding:. In commit stage: $\forall\ \mathsf{R}^*$, $m \in \mathbb{N}$ and $b \neq b' \in \{0,1\}^m$,
$\{\mathrm{View}_{\mathsf{R}^*}(\mathsf{S}(b), \mathsf{R}^*)(1^n)\}_{n\in\mathbb{N}} \approx_c \{\mathrm{View}_{\mathsf{R}^*}(\mathsf{S}(b'), \mathsf{R}^*)(1^n)\}_{n\in\mathbb{N}}$.

Commitment Schemes cont.

Binding: “Any" S^* succeeds in the following game with negligible probability in n:

> *On security parameter* 1^n, S^* *interacts with* R *in the commit stage resulting in a commitment* c*, and then output two pairs* (d, b) *and* (d', b') *with* $b \neq b'$ *such that* $\mathsf{R}(c, d, b) = \mathsf{R}(c, d', b') = \texttt{Accept}$

Commitment Schemes cont.

- wlg. we can think of d as the random coin of S, and c as the transcript
- Hiding: Perfect, statistical, computational
- Binding: Perfect, statistical. computational
- Cannot achieve both properties to be statistical simultaneously.
- For computational security, we will assume non-uniform entities:
  On security parameter n, the adversary gets an auxiliary input z_n (length of auxiliary input does not count for the running time)
- Suffices to construct “bit commitments"
- (non-uniform) OWFs imply statistically binding, and statistically hiding commitments

Perfectly Binding Commitment from OWP

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ be a permutation and let P be a (non-uniform) hardcore predicate for f

Protocol 2 ((S,R))

Commit:

S's input: $b \in \{0,1\}$

S chooses a random $x \in \{0,1\}^n$, and sends $c = (f(x), P(x) \oplus b)$ to R

Reveal:

S sends (x,b) to R, and R accepts iff (x,b) is consistent with c (i.e., $P(x) \oplus b = c$)

Perfectly Binding Commitment from OWP cont.

Claim 3

The above protocol is perfectly binding (and computationally hiding) commitment

Proof: Correctness and binding are clear.

Hiding: for any (possibly non-uniform) algorithm A, let

$$\Delta_n^A = |\Pr[A(f(U_n), P(U_n) \oplus 0) = 1] - \Pr[A(f(U_n), P(U_n) \oplus 1) = 1]|$$

It follows that

$$|\Pr[A(f(U_n), P(U_n) \oplus 0) = 1] - \Pr[A(f(U_n), P(U_n) \oplus U) = 1]| = \Delta_n^A/2$$

Hence,

$$|\Pr[A(f(U_n), P(U_n)) = 1] - \Pr[A(f(U_n), U) = 1]| = \Delta_n^A/2 \quad (1)$$

Thus, Δ_n^A is negligible for any PPT

Statistically Binding Commitment from OWF.

Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{3n}$ be a (non-uniform) PRG

Protocol 4 ((S,R))

Commit

Common input: 1^n

S's input: $b \in \{0,1\}$

Commit:

1. R chooses a random $r \leftarrow \{0,1\}^{3n}$ to S
2. S chooses a random $x \in \{0,1\}^n$, and send $g(x)$ to S in case $b = 0$ and $c = g(x) \oplus r$ otherwise.

Reveal: S sends (b,x) to R, and R accepts iff (b,x) is consistent with r and c

Correctness is clear. Hiding and biding HW